Simple Groups from Order 201 to Order 500.

By F. N. Cole, Ph. D.

In a recent number of the Mathematische Annalen* Dr. Otto Hölder has determined all the simple groups as far as order 200. The importance of this class of groups and the lack of any general method for their construction render it desirable to extend this census as far as possible. Only the simple groups furnish new algebraic problems, the reduction of a compound group being effected by means of a series of simple groups of lower orders. The number of simple groups is very limited. Beside the (necessarily cyclical) groups of prime order, which are always simple, Dr. Hölder finds below order 201 only two other cases, both of which have long been known, viz., a simple group of order 60, isomorphic with the alternating group of permutations of 5 letters, and a simple group of order 168, isomorphic with the group identified with the transformation of the 7th order of the elliptic modular functions.

From order 201 to order 500 there is one known simple group of order 360, isomorphic with the alternating group of permutations of 6 letters. Beside this I find only two other possibilities of compound order, both of which present more serious difficulties than I have as yet been able to meet. I do not here prove or disprove the existence 1) of a second simple group of order 360 not isomorphic with the group of even permutations of 6 letters, or 2) of a simple group of order 432. It seems, however, a measurable advance to have restricted the necessity of further consideration to these two cases.

I.—*Preliminary Theorems.*

The general method here employed is identical with that of Dr. Hölder's article, to which and to the works of Netto and Serret the reader is referred for further particulars. It is to be especially noted that, the simple or compound

*Math. Ann. XL, 1, p. 55.

character being a property of a group in itself, independent of the particular form in which its operations are expressed, we deal here primarily with groups in the abstract, only recurring when convenient to their representation in terms of substitutions of n letters.

In the analysis of the structure of a group the theorems of Sylow* are indispensable:

I.—*A group the order of which is a power of a prime number is compound.*

II.—*If p^a is the highest power of a prime number p which divides the order r of a group G, then the subgroups of order p^a contained in G are all conjugate, and their number is $\varkappa p+1$, where*

$$r = p^a . \nu . (\varkappa p + 1),$$

the integers ν and $\varkappa$ remaining to be determined in each particular case.

From these Dr. Hölder deduces the two following:

III.—*If the order of a group is a product of two or of three prime factors, including the case where any of the factors are equal, the group is compound.*

IV.—*If the group G of Theorem II is simple, it is holoedrically isomorphic with a transitive group of substitutions of $\varkappa p + 1$ letters.*

It follows at once from the last Theorem that the order r of G must be a divisor of $(\varkappa p+1)!$ Also, since there is only one group of substitutions of 6 letters, the alternating group of order 360, the order of which lies between 201 and 500, we must always have $\varkappa p + 1 > 6$, except when $r = 360$.

The following well known theorem† is also of great use for the present purpose:

V.—*If a transitive group G of substitutions of n letters contains a transitive subgroup of lower degree, then G is either doubly transitive or non-primitive.*

It is to be noted further that if a simple group G of an order above 120 is non-primitive, its number of systems of non-primitivity must exceed 6. Otherwise it would be possible‡ to construct a simple group of substitutions holoedrically isomorphic with G and affecting not more than 6 letters.

Finally, a simple group G, expressed in substitutions, cannot contain any odd substitution. For the even substitutions would then give a self-conjugate subgroup.||

* L. Sylow: Math. Ann., V, p. 284.

† Cf. Netto: Theory of Substitutions, p. 95, Corollary.

‡ Ibid., p. 76.

|| Ibid., pp. 35 and 81.

II.—*First Reduction of the Number of Possible Orders.*

Between 201 and 500 I find the following 84 numbers which are not powers of a single prime or products of two or of three primes:

$* 204 = 2^2 . 3 . 17$	$* 312 = 2^3 . 3 . 13$	$* 408 = 2^3 . 3 . 17$
$* 208 = 2^4 . 13$	$315 = 3^2 . 5 . 7$	$* 414 = 2 . 3^2 . 23$
$210 = 2 . 3 . 5 . 7$	$** 320 = 2^5 . 5$	$* 416 = 2^5 . 13$
$** 216 = 2^3 . 3^3$	$** 324 = 2^2 . 3^4$	$420 = 2^2 . 3 . 5 . 7$
$* 220 = 2^2 . 5 . 11$	$* 328 = 2^3 . 41$	$* 424 = 2^3 . 53$
$\dagger 224 = 2^5 . 7$	$* 330 = 2 . 3 . 5 . 11$	$432 = 2^4 . 3^3$
$* 225 = 3^2 . 5^2$	$336 = 2^4 . 3 . 7$	$* 440 = 2^3 . 5 . 11$
$* 228 = 2^2 . 3 . 19$	$* 340 = 2^2 . 5 . 17$	$* 441 = 3^2 . 7^2$
$* 232 = 2^3 . 29$	$* 342 = 2 . 3^2 . 19$	$* 444 = 2^2 . 3 . 37$
$* 234 = 2 . 3^2 . 13$	$* 344 = 2^3 . 43$	$\dagger 448 = 2^6 . 7$
$240 = 2^4 . 3 . 5$	$* 348 = 2^2 . 3 . 29$	$** 450 = 2 . 3^2 . 5^2$
$* 248 = 2^3 . 31$	$* 350 = 2 . 5^2 . 7$	$* 456 = 2^3 . 3 . 19$
$* 250 = 2 . 5^3$	$351 = 3^3 . 13$	$* 459 = 3^3 . 17$
$252 = 2^2 . 3^2 . 7$	$* 352 = 2^5 . 11$	$* 460 = 2^2 . 5 . 23$
$* 260 = 2^2 . 5 . 13$	$360 = 2^3 . 3^2 . 5$	$* 462 = 2 . 3 . 7 . 11$
$264 = 2^3 . 3 . 11$	$* 364 = 2^2 . 7 . 13$	$* 464 = 2^4 . 29$
$** 270 = 2 . 3^3 . 5$	$* 368 = 2^4 . 23$	$* 468 = 2^2 . 3^2 . 13$
$* 272 = 2^4 . 17$	$* 372 = 2^2 . 3 . 31$	$* 472 = 2^3 . 59$
$* 276 = 2^2 . 3 . 23$	$* 375 = 3 . 5^3$	$* 476 = 2^2 . 7 . 17$
$280 = 2^3 . 5 . 7$	$* 376 = 2^3 . 47$	$480 = 2^5 . 3 . 5$
$288 = 2^5 . 3^2$	$* 378 = 2 . 3^3 . 7$	$* 484 = 2^2 . 11^2$
$* 294 = 2 . 3 . 7^2$	$380 = 2^2 . 5 . 19$	$* 486 = 2 . 3^5$
$* 296 = 2^3 . 37$	$** 384 = 2^7 . 3$	$* 488 = 2^3 . 61$
$* 297 = 3^3 . 11$	$* 390 = 2 . 3 . 5 . 13$	$* 490 = 2 . 5 . 7^2$
$** 300 = 2^2 . 3 . 5^2$	$\dagger 392 = 2^3 . 7^2$	$* 492 = 2^2 . 3 . 41$
$* 304 = 2^4 . 19$	$396 = 2^2 . 3^2 . 11$	$495 = 3^2 . 5 . 11$
$306 = 2 . 3^2 . 17$	$400 = 2^4 . 5^2$	$* 496 = 2^4 . 31$
$* 308 = 2^2 . 7 . 11$	$* 405 = 3^4 . 5$	$* 500 = 2^2 . 5^3$

Of these those marked * or ** are to be rejected, the former because for one or another factor p the number $xp + 1$ can only be 1, the latter because $xp + 1$ is less than 7. Further, the three cases 224, 392, and 448 are excluded, since these orders are not divisors of corresponding numbers $(xp + 1)!$. The possible simple groups are therefore included among the following 18 orders:

$210 = 2.3.5.7$	$306 = 2.3^2.17$	$396 = 2^2.3^2.11$
$240 = 2^4.3.5$	$315 = 3^2.5.7$	$400 = 2^4.5^2$
$252 = 2^2.3^2.7$	$336 = 2^4.3.7$	$420 = 2^2.3.5.7$
$264 = 2^3.3.11$	$351 = 3^3.13$	$432 = 2^4.3^3$
$280 = 2^3.5.7$	$360 = 2^3.3^2.5$	$480 = 2^5.3.5$
$288 = 2^5.3^2$	$380 = 2^2.5.19$	$495 = 3^2.5.11$

III.—*Further Reduction of the* 18 *Cases to* 7.

1. Of the remaining 18 orders the following 7 are at once disposed of:

240, 280, 306, 351, 380, 396, 495.

Thus, if $r = 240 = 5.\nu.(5x + 1)$, we must take $5x + 1 = 6$ or 16. 6 is excluded. A simple group of order 240 must therefore be isomorphic with a transitive group of 240 substitutions of 16 letters. The subgroup which leaves one of the 16 letters unchanged is then of order $\frac{240}{16} = 15$. But a group of order 15 is necessarily cyclical; its operations are all powers of a single one among them, s_1. The powers of s_1, the exponents of which are divisible by 3, form a self-conjugate subgroup of order 5. Every operation of this subgroup, except identity, must consist of exactly 3 cycles of five letters each. Otherwise the same subgroup of order 5 would occur in several of the groups which leave a single one of the 16 letters unchanged, and there would therefore be less than 16 subgroups of order 5. The operation s_1 accordingly cannot consist of cycles of 5 letters with cycles of 3 letters, but must be a single cycle of 15 letters. Every power of s_1 therefore affects all the 15 letters. The group of order 240 then contains $16.14 = 224$ distinct operations of order 15, leaving only 16 further operations. There can therefore be only *one* subgroup of order 16. Consequently a group of order 240 is compound.

Again, if $r = 280 = 7.\nu.(7x + 1)$, we have $7x + 1 = 8$. There is therefore to be a simple transitive group of 280 substitutions of 8 letters. This requires a subgroup of order 35 affecting 7 letters. But a group of order 35 is cyclical, and such a group cannot be constructed with 7 letters.

For $r = 306 = 17.\nu.(17x + 1)$ we have $17x + 1 = 18$, and a simple transitive group of 306 substitutions of 18 letters, with 18 subgroups of order 17 affecting 17 letters. These give $18.16 = 288$ operations of order 17, leaving

only 18 further operations, each of which must affect all the 18 letters. Among these there must be a substitution of order 2, which must then consist of 9 cycles of two letters each. But such a substitution is odd.

For $r = 351 = 13.\nu.(13x + 1)$ there must be 27 subgroups of order 13, involving $27.12 = 324$ distinct operations. There remain only 27 further operations, which can furnish only *one* group of order 27.

For $r = 380 = 19.\nu.(19x + 1)$ we have 20 subgroups of order 19, with $20.18 = 360$ distinct operations. Also from $380 = 5.\nu.(5x + 1)$ it follows that there are 76 subgroups of order 5, with 76.4 further operations. But these cannot all be included in a group of order 380.

If $r = 396 = 11.\nu.(11x + 1)$, there must be a simple transitive group of 396 substitutions of 12 letters, containing 12 subgroups of order 33 affecting 11 letters. But a group of order 33 is cyclical, and is impossible with only 11 letters.

Finally, if $r = 495 = 11.\nu.(11x + 1)$, we have 45 subgroups of order 11, containing $45.10 = 450$ distinct operations of order 11. But from $495 = 5.\nu.(5x + 1)$ it appears that there are also 11 subgroups of order 5, containing $11.4 = 44$ operations of order 5. These two sets of operations together with identity make up the entire group, leaving no opportunity for any operations of order 3.

The 7 orders just discussed therefore afford no simple groups.

2. Of the 11 cases remaining, the following 4 also present no considerable difficulty:

210, 264, 315, 336.

For $r = 210 = 7.\nu.(7x + 1)$ there must be 15 subgroups of order 7, containing $15.6 = 90$ distinct operations of this order. Also from $210 = 3.\nu.(3x + 1)$ we have $3x + 1 = 7$, 10, or 70. In the last case there would be $70.2 = 140$ operations of order 3, which could not all be included in the group. Also if $3x + 1 = 7$, there must be a simple transitive group of 210 substitutions of 7 letters. This would contain subgroups of order 30, affecting 6 letters. But a group of order 30 contains a cyclical subgroup of order 15, and this cannot be constructed with 6 letters. Finally, if $3x + 1 = 10$, the isomorphic group of 210 substitutions of 10 letters would include a circular substitution of 7 letters, and must therefore be doubly transitive or non-primitive. Both of these possibilities are here excluded. There is therefore no simple group of this order.

Again, if $r = 264 = 11.\nu.(11x + 1)$, we require a simple, transitive group of 264 substitutions of 12 letters. This will include 12 subgroups of order 22, affecting 11 letters. Such a subgroup consists of the powers of a circular substitution of 11 letters and 11 substitutions with 5 cycles of two letters each. The latter substitutions being odd, there is no simple group of this order.

If $r = 315 = 9.\nu.(3x + 1)$, there must be a simple, transitive group of 315 substitutions of 7 letters. This group must contain a circular substitution of 5 letters. But the group is neither doubly transitive nor non-primitive.

For $r = 336 = 7.\nu.(7x + 1)$, we must have $7x + 1 = 8$. The corresponding simple, transitive group of 8 letters contains subgroups of 42 substitutions of 7 letters. Such a subgroup contains a further, self-conjugate subgroup of order 7, consisting of the powers of a circular substitution of 7 letters. It contains further an operation of order 2. This operation cannot consist of 1 or of 3 cycles of two letters, since both of these cases are odd. But 2 cycles of two letters cannot transform the circular substitution of 7 letters into any of its powers, as must here be the case.

IV.—*The Orders* 252, 288, 400, 420, *and* 480.

These require a more detailed consideration, involving a somewhat elaborate determination of the possible orders of the included operations.

1. $r = 252$. This case requires 36 subgroups of order 7, furnishing at once $36.6 = 216$ of the 252 operations. The corresponding simple, transitive group of 36 letters contains 36 subgroups of order 7 affecting 35 letters each. Every actual substitution of these subgroups must consist of 5 cycles of 7 letters each; otherwise there would not be 36 *distinct* subgroups of this type. The remaining 35 actual substitutions affect all the 36 letters. Every one of them must be regular, i. e. must consist of cycles all of which contain the same number of letters. Otherwise a proper power of one of them would affect less than 35 letters, without being identity.

There can be no operation of order 9 in the group. For such an operation must consist of 4 cycles of 9 letters each. An operation of order 7 could not transform this operation into itself or into any of its powers. Every operation of order 9 would therefore give rise, on being transformed by an operation of order 7, to 7 conjugate operations of order 9. The 1st, 2d, 4th, 5th, 7th, and

8th powers of these 7 operations must all be distinct. We should have therefore $7.6 = 42$ distinct new operations, whereas there can be only 36. There is therefore no operation of order 9, 18, or 36 in the group.

The possible orders beside 7, which must all be divisors of 36, are therefore reduced to 12, 6, 4, 3, and 2. An operation of order 12 must consist of 3 cycles of 12 letters each, and one of order 4 of 9 cycles of 4 letters each. Both of these cases are odd. There therefore remain only the orders 2, 3, and 6. The substitutions of these orders, like the hypothetical substitutions of order 9, must be joined in conjugate sets of 7 each. At least one subgroup of order 2 and one of order 3 are present. These give rise to at least 7 operations of order 2 and $7.2 = 14$ of order 3. If any operation of order 6 is present this gives rise to 7 conjugate groups of this order, the first and fifth powers of whose generating substitutions are all distinct. These would furnish the $7.2 = 14$ missing operations.

On the other hand, if no operation of order 6 is present, then no operation of order 3 can transform an operation of order 2 into itself. For in this case the product of the two operations would be of order 6. Consequently the number of the operations of order 2 is a multiple of 3 as well as of 7, and is therefore a multiple of 21. There are therefore at least 21 operations of order 2 in the group. These, with the 14 necessarily present operations of order 3 and identity, make up the 36 operations to be supplied.

In any case, then, the group contains exactly 14 operations of order 3. From these 14 operations at least 7 subgroups of order 9 are to be constructed. These groups consist of 8 commutative operations of order 3 and identity. Two such groups, if distinct, cannot have more than 3 operations in common. In the present case they must have 3 operations in common; otherwise they would furnish 16 operations of order 3. If they have 3 operations in common they furnish together all the 14 possible operations of order 3. A third group of order 9 must therefore have all its operations in common with these two. But it can have only 3 (including identity) in common with each, or 5 with both. Accordingly, from the 14 operations of order 3 only two (if any) groups of order 9 can be constructed. A group of order 252 is therefore simple.

2. $r = 288$. We must have here 9 conjugate subgroups of order 32. There is therefore to be a simple, transitive group of 288 substitutions of 9 letters.

The 9 subgroups which affect 8 letters are those of order 32. The operations of such a group are of orders 32, 16, 8, 4, and 2; 32 and 16 are here excluded. Also a circular substitution of 8 letters, being odd, is inadmissible. Every operation of the subgroups of order 32 therefore consists of cycles of 4 and of 2 letters; 1 cycle of 4 letters, or 1 or 3 cycles of two letters are odd; 2 cycles of 2 letters cannot occur in a primitive group of degree 9; 1 cycle of 4 letters with 1 of 2 letters is excluded, since its square would have 2 cycles of 2 letters. There remain only substitutions of 2 cycles of 4 letters, or 4 cycles of 2 letters. Every substitution of the 9 subgroups of order 32 therefore affects all the 8 letters. These subgroups accordingly furnish $9.31 = 279$ distinct substitutions, leaving only 9. The latter can form at the most *one* subgroup of order 9.

3. $r = 400$. In this case there must be 16 conjugate subgroups of order 25, and therefore a simple, transitive group of 400 substitutions of 16 letters. The subgroups which leave one letter unchanged are the 16 subgroups of order 25. These cannot be cyclical, since they affect only 15 letters. Any one of them therefore consists of 24 commutative substitutions of order 5 and the identical substitution. Suppose that s_1 and s_2 are any two of the substitutions of such a group. Then s_2 transforms s_1 into itself, and since s_1 contains at the most 3 cycles, s_2 must transform every cycle of s_1 into itself. Consequently the cycles of s_2 are powers of cycles of s_1 so far as s_1 and s_2 have letters in common. It follows that the 15 letters affected by the group divide into 3 transitive systems of 5 letters each, and that every substitution of the group is a combination of one, two, or three circular substitutions u, v, w, of order 5, each of which affects one of the three systems of transitivity.

No substitution of the group of order 400 can consist of a single cycle of 5 letters. For the group would then be non-primitive. The only admissible distribution of the 16 letters would be into 8 systems of 2 letters each. But 400 is not a divisor of $2^8 . 8!$ Also the substitutions of the subgroup of order 25 cannot all consist of three cycles each. For then these subgroups would furnish $16 . 24 = 384$ distinct operations, leaving only 16, from which only *one* subgroup of order 16 could be formed.

A subgroup of order 25 therefore contains some operations with two cycles of 5 letters. Suppose one of these to be uv. There can then be no other operation $u^i v^j (i \neq j)$ in the group, for $(uv)^{-i} u^i v^j$ would consist of a single cycle.

The 5 powers of uv cannot make up the entire subgroup. We must therefore add to these some uw, or vw, or $uv^\lambda w^\mu$. Whatever choice is made, there is essentially only one result. The subgroup must contain the combinations

$$uv, \quad uw, \quad vw^4,$$
$$uv^2w^4, \quad uv^3w^3, \quad uv^4w^2.$$

These with their powers furnish all the $6.4+1=25$ operations of the subgroup.

The group of order 400 contains therefore $\frac{16}{6}.12=32$ substitutions of order 5 with two cycles. These divide into 8 groups. There must therefore be a simple, transitive group of 400 substitutions of, at the most, 8 letters. But such a group is impossible, since 400 is not a divisor of $8\,!$.

4. $r=420$. Here $7x+1$ must equal 15. We require therefore a simple, transitive group of 420 substitutions of 15 letters. A subgroup which leaves one letter unchanged is of order 28, and therefore contains an operation of order 7. This cannot be a circular substitution; it consists then of two cycles of 7 letters each. The subgroup composed of the powers of this operation is self-conjugate in respect to the group of order 28. Of the remaining 21 operations of this group none can be of order 14 or 28. For a cycle of 14 letters is odd, and any combination of a cycle of 7 letters with one of 2 or 4 letters contains among its powers a single cycle of 7 letters.

All the 21 remaining operations are therefore of order 2 or order 4. One of order 4 is inadmissible, for an operation of order 4 cannot transform an operation of order 7 into any of its powers except the first. And in the latter case the product of the two operations would be of order 28. Also the operations of order 2 cannot transform the operation of order 7 into itself, for then we must have operations of order 14. Consequently every operation σ of order 2 must transform the operation s of order 7 into its 6^{th} power; σ cannot interchange the two cycles of s, for then σ must consist of 7 cycles of two letters. Accordingly σ leaves 1 letter of each cycle of s unchanged, and interchanges the remaining 6 letters of each cycle in pairs. As soon as the two fixed letters are assigned, σ is fully determined. Moreover, a given letter of the one cycle cannot be paired as fixed letter with two different letters of the other cycle. For then the product of the two corresponding substitutions of order 2 would be different

from identity, but would not affect the letters of the first cycle of s, and could not therefore transform this cycle into its 6^{th}-power. It is therefore possible to construct only 7 of the 21 required substitutions of order 2.

There is then no simple group of order 420.

5. $r = 480$. We must have here either 16 or 96 subgroups of order 5. In the former case the corresponding group of substitutions of 16 letters contains subgroups of order 30, affecting 15 letters. Each of these subgroups contains a self-conjugate subgroup of order 5. Every actual operation of the latter consists of 3 cycles of 5 letters each; otherwise the group of order 480 would not contain 16 subgroups of order 5. A group of order 30 contains, moreover, a cyclical subgroup of order 15, the generating operation of which must here consist of a single cycle of 15 letters, since its 3^d power is of order 5. The remaining substitutions of the group of order 30 are of order 2, and each consists of 7 cycles of 2 letters each, and is therefore odd. Consequently a simple group of order 480 contains 96 subgroups of order 5. These furnish $96 . 4 = 384$ distinct operations of order 5, leaving $96 - 1$ to be identified.

The number of subgroups of order 3 cannot now exceed 48. Below this limit we find $3x + 1 = 10$, 16, or 40. The last two numbers are impossible. For 40 subgroups of order 3 would furnish 80 operations, leaving only 16 from which to form groups of order 32. And 16 groups of order 3 would require a simple, transitive group of 480 substitutions of 16 letters, which, we have just shown, does not exist. There are therefore exactly 10 subgroups of order 3. The corresponding group of substitutions of 10 letters contains 10 conjugate subgroups of order 48, affecting 9 letters. Each of these contains again 1 or 3 subgroups of order 16. We show that every actual substitution of such a subgroup affects exactly 8 letters.

In the first place there can obviously be no operation of order 16 present. Also an operation of order 8 must here consist of a single cycle of 8 letters, which, being odd, is also excluded. Every operation of the groups of order 16 under consideration must therefore be of order 4 or order 2; 1 or 3 cycles of 2 letters, 1 cycle of 4 letters, and one cycle of 4 with 2 of 2 are excluded, being odd; 2 cycles of 2 letters are also excluded. There remain only 2 cycles of 4 letters, 4 cycles of 2 letters, and 1 cycle of 4 letters with one of 2 letters. The last case is also excluded, since the square of such a substitution would consist of 2 cycles

of 2 letters. Every substitution of the groups of order 16 therefore affects 8 letters. The 8 letters are the same for every substitution of the same group. For if we multiply 4 cycles of 2 letters into 4 cycles of 2 letters having 7 letters in common with the first set, it is impossible to remove one letter, without removing two.

Now a primitive group of substitutions of n letters contains a subgroup actually affecting any $n - 1$ letters.* If a subgroup of order 16 contained in a group of order 48 is transformed by a proper operation of the group affecting all the 9 corresponding letters, the result is a new subgroup of order 16 affecting a different 8 of the 9 letters. Each group of order 48 therefore contains more than 1 subgroup of order 16, and therefore contains 3 such subgroups. Each of these subgroups, leaving 2 of the 10 letters unchanged, occurs in two of the groups of order 48. There are therefore $\frac{10}{2} . 3 = 15$ subgroups of order 16. The actual operations of these groups must all be different, since each group affects a different set of 8 letters. They furnish therefore $15 . 15 = 225$ new operations, whereas only 75 are admissible.

There is, then, no simple group of order 480, and the possible orders of simple groups of compound order between 201 and 500 are reduced to 360 and 432.

ANN ARBOR, *June*, 1892.

---

*Netto: p. 94, Theorem XXII.